IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPEAL NO:

In Re Application of: Mark E. ROSE

Confirmation No.: 1899

Serial No.: 09/832,683

Filed: April 10, 2001

For: ACCESS CONTROL FOR DISTRIBUTED CONTENT SERVERS

APPEAL BRIEF

Stephen G. Sullivan
Attorney for Appellants
Strategic Patent Group P.C.
475 N. Whisman Rd, Suite 400
Mountain View, CA 94043

TOPICAL INDEX

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicant(s): Mark E. ROSE	Date: September 11, 2007
Serial No.: 09/832,683	Group Art Unit: 2145
Filed: 4/10/2001	Examiner: Choudhury, Azizul Q.
Title: Access Control for Distributed Content Servers	Confirmation No.: 1899

Mail Stop Appeal Briefs-Patents
Commissioner of Patents
P. O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Appellant herein files an Appeal Brief drafted in accordance with the provisions of 37 C.F.R. §41.37 as follows:

I REAL PARTY IN INTEREST

Appellant respectfully submits that the above-captioned application is assigned, in its entirety to SumTotal Systems, Inc. of Mountain View, California.

II RELATED APPEALS AND INTERFERENCES

Appellant states that, upon information and belief, he is not aware of any co-pending appeal or interference which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III STATUS OF CLAIMS

Application Serial No. 09/832,683 (the instant application), as originally filed, included claims 1-38. Claims 1, 3-6, 8-10, 12-13, 15-18, 20-22, 24-25, 27-30, 32-34, and 36 are presently pending.

In response to a Non-Final Office Action (dated November 2, 2004), an Amendment (dated February 2, 2005) was filed with claims 1, 10, and 13 amended.

In response to a Non-Final Office Action (dated May 19, 2005), an Amendment (dated November 21, 2005), was filed with claims 1, 8, 10, 13, 20, 26-30, and 32-36 amended and claims 7, 19, and 31 canceled.

In response to a Non-Final Office Action (dated August 28, 2006), an Amendment (dated November 27, 2006) was filed with claims 1, 13, 25, and 34 amended and claims 2, 11, 14, 23, 35, 37, and 38 canceled.

In response to a Final Office Action (dated March 14, 2007), a Response (dated May 14, 2007) was filed with no claims amended, cancelled, or added.

Claims 1, 3-6, 8-10, 12-13, 15-18, 20-22, 24-25, 27-30, 32-34, and 36 remain rejected. Claims 1, 3-6, 8-10, 12-13, 15-18, 20-22, 24-25, 27-30, 32-34, and 36 are on appeal and all applied prospective rejections concerning Claims 1, 3-6, 8-10, 12-13, 15-18, 20-22, 24-25, 27-30, 32-34, and 36 are being appealed herein.

IV STATUS OF AMENDMENTS

The Response submitted in response to the Final Office Action dated May 14, 2007 did not amend, cancel, or add any claims.

V SUMMARY OF CLAIMED SUBJECT MATTER

The invention provides a method, system, and computer readable medium with program instructions for controlling access to files on a server over a method. Independent claim 1 and 25 recite the method and computer readable medium with program instructions comprising: allowing a content originator to publish a file on a first server (content server 24; Fig. 2) and to specify what users are authorized to access to file (p. 11, lines 3-6; Fig. 4); replicating the file from the first server on a second server (replica server 26; Fig. 2; p. 11, lines 6-7); in response to receiving a URL request from a client for a file from the first server, determining if a user of the client has been granted authorization to access the file (p. 11, lines 8-11; p. 12, line 22 – p. 13, line 7), wherein a client address apparent to the first server differs from a client address apparent to the second server (p. 1, lines 11-15; p. 14, line 19 – p. 15, line 1); generating a transfer ticket from the first server to the client that includes an identifier identifying the particular file on the second server if the user has been granted authorization access (p. 11, lines 11-14; p. 13, lines 8-15), wherein the transfer ticket is not bound to the client address apparent to the first server (p. 17, lines 8-16); in response to receiving the transfer ticket from the client by the second server, redirecting the client back to the second server with a URL ticket (p. 11, lines 15-18; p. 17, lines 20-23), wherein the URL ticket is bound to the client address apparent to the second server (p. 14, line 6 – p. 15, line 13; Fig. 5, clientid parameter); and in response to receiving the URL ticket from the client, verifying the URL ticket on the second server and returning the file (p. 11, lines 21 – p. 12, line 2).

Independent claim 13 recites the system, comprising: means for allowing a content originator to publish a file on a first server and to specify what users are

authorized to access to the file, wherein files on the first server are replicated on a second server (content server 24 and replica server 26 running software; Fig. 2; p. 11, lines 3-6; Fig. 4; p. 11, lines 6-7); means responsive to receiving a URL request from a client for a file from the first server for determining if a user of the client has been granted authorization to access the file (content server 24 running software; p. 11, lines 8-11; p. 12, line 22 – p. 13, line 7), wherein a client address apparent to the first server differs from a client address apparent to the second server (p. 1, lines 11-15; p. 14, line 19 – p. 15, line 1); means for generating a transfer ticket from the first server to the client that includes an identifier identifying the particular file on the second server if the user has been granted authorization access (content server 24 running software; p. 11, lines 11-14; p. 13, lines 8-15), wherein the transfer ticket is not bound to the client address apparent to the first server (p. 17, lines 8-16); means for receiving the transfer ticket from the client by the second server and redirecting the client back to the second server with a URL ticket (replica server 26 running software; p. 11, lines 15-18; p. 17, lines 20-23), wherein the URL ticket is bound to the client address apparent to the second server (clientid parameter; Fig. 5; p. 14, line 6 – p. 15, line 13); and means for verifying the URL ticket on the second server and returning the file (replica server 26 running software; p. 11, lines 21 – p. 12, line 2).

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 13, and 25 stand rejected under 35 U.S.C. §112, first paragraph as failing to comply with the enablement requirement.

Claims 1, 3-6,8-10, 12-13, 15-18, 20-22, 24-25, 27-30, 32-34, and 36 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Levergood et al (5,708,780) in view of the FileNet Functionality Sheet (hereinafter referred to as Levergood and FileNet, respectively).

VII ARGUMENTS

1. Rejection of claims 1, 13, and 25 under 35 U.S.C. §112, first paragraph, failing to comply with the enablement requirement

In the Final Office Action dated March 14, 2007, the Examiner states, "The claim amendments now state that the second server sends the transfer ticket, received by the client. However, the specifications and drawings teach that the first server sends the transfer ticket received by the client."

Appellant respectfully disagrees with the Examiner's reading of claims 1, 13, and 25. Claims 1, 13, and 25 do not recite that the second server generates the transfer ticket. Instead, these claims recite that the transfer ticket is generated *from the first server to the client*. The second server is recited as *receiving the transfer ticket from the client*. The Examiner's reading is contrary to the plain language of claims 1, 13, and 15, and these claims are fully supported by the specification.

Accordingly, Appellant respectfully requests withdrawal of the rejection under 35 U.S.C. 112, first paragraph, and respectfully requests that the Board reverse the final rejection of claims 1, 13, and 25.

2. Rejection of 1, 3-6, 8-10, 12-13, 15-18, 20-22, 24-25, 27-30, 32-34, and 36 under 35 U.S.C. §103(a) as being unpatentable over Levergood et al (5,708,780) view of the FileNet Functionality Sheet

It is respectfully submitted that Levergood in view of FileNet fails to teach or suggest each and every element of independent claims 1, 13, and 25.

In a network environment where the client address apparent to the first server differs from the client address apparent to the second server, the invention, as recited in independent claims 1, 13, and 25, addresses the problem of restricting access in

such an environment by the use of transfer tickets in combination with URL requests. In response to receiving a URL request from the client, the first server determines if the use of the client has been granted authorization to access the file. The first server generates the transfer ticket to the client that includes an identifier identifying the particular file on the second server if the user has been granted authorization access. The transfer ticket is not bound to the client address apparent to the first server. In response to receiving the transfer request from the client, the second server redirects the client back to itself with a URL ticket that is bound to the client address apparent to the second server. When the second server receives the URL ticket from the client, it verifies the URL ticket and returns the file.

In this manner, it is ensured that only the client that was issued the URL ticket can use the URL ticket to access the file, even though the client address apparent to the first and second servers are different. Neither active communication between the first server and the second server is required, nor the duplication of authentication and access control information on both the first and second servers.

Levergood discloses a client request made with a URL from a web browser. A content server redirects the client to an authentication server. The authentication server interrogates the client and then issues an SID to a qualified client. A valid SID typically comprises a user identifier, an accessible domain, a key identifier, an expiration time, the IP address of the user computer, and a digital signature. The authentication server then forwards a new request consisting of the original URL appended by the SID to the client in a Redirect. The modified request formed by a new URL is automatically forwarded by the client browser to the content server. When the

content server receives a URL request accompanied by an SID, it logs the URL with the SID and the user IP address in a transaction log and proceeds to validate the SID. When the SID is so validated, the content server sends the requested document for display by the client's web browser. (Col. 3, lines 21 – 49)

Levergood, however, does not address a situation where the file is replicated from the content server on a replica server, where the file is to be returned to the client from the replica server, and where the client address apparent to the content server differs from a client address apparent to the replica server. The mechanism in Levergood addresses the problem where the IP address of the user computer may not be known to the content server by issuing the SID as described above. Levergood, however, does not disclose how the file can be returned to the client by the replica server when the client address apparent to the content server differs from a client address apparent to the replica server. The mechanism disclosed in Levergood would be inadequate in this situation. Although Levergood discloses an authentication server, Levergood does not disclose replication of files on the authentication server. The authentication server thus is not analogous to the recited second server.

Further, Levergood does not disclose the generation of a transfer ticket that is not bound to the client address apparent to the first server. Levergood instead discloses the authentication server issuing of a valid SID that comprises "a user identifier, an accessible domain, a key identifier, an expiration time such as date, the *IP address of the user computer*, and an unforgettable digital signature…The authentication server then forwards a new request consisting of the original URL appended by the SID to the client in a REDIRECT. The modified request formed by a

new URL is automatically forwarded by the client browser to the content server." (Col. 3, lines 33-47) Since the SID includes the IP address of the user computer, the modified request formed by the new URL that is forwarded to the content server is bound to the client address apparent to the first server.

For these reasons, Levergood fails to teach or suggest a transfer ticket that is not bound to the client address apparent to the first server and a URL ticket that is bound to the client address apparent to the second server.

A secondary reference stands or falls with the primary reference. Because Levergood fails to teach or suggest a transfer ticket that is not bound to the client address apparent to the first server and a URL ticket that is bound to the client address apparent to the second server, a combination of Levergood with FileNet also fails to teach or suggest the claimed invention. Accordingly, claims 1, 13, and 25 are patentable over these references. Claims 3-6, 8-10, 12, 15-18, 20-22, 24, 27-30, 32-34, and 36 are allowable because they depend upon these allowable independent claims.

Accordingly, Appellant respectfully requests withdrawal of the rejection under 35 U.S.C. 103(a) and respectfully requests that the Board reverse the final rejection of claims 1, 3-6, 8-10, 12-13, 15-18, 20-22, 24-25, 27-30, 32-34, and 36.

For all the foregoing reasons, it is respectfully submitted that Claims 1, 3-6, 8-10, 12-13, 15-18, 20-22, 24-25, 27-30, 32-34, and 36 (all the Claims presently in the application) are patentable. Thus, Appellant respectfully requests that the Board reverse the rejection of the appealed Claims and find each of these Claims allowable.

Note: For convenience of detachment without disturbing the integrity of the remainder of pages of this Appeal Brief, Appellant's

"APPENDIX" sections are contained on separate sheets following the signatory portion of this Appeal Brief.

CERTIFICATE
I hereby certify that this correspondence is being facsimile or electronically transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below
Date: September 11, 2007

Signature: /Stephen G. Sullivan/
Typed Name: Stephen G. Sullivan

Respectfully submitted,

/Stephen G. Sullivan/
Stephen G. Sullivan
Attorney/Agent for Applicant(s)
Reg. No. 38329
Telephone No.: 650 969-7474

Date: September 11, 2007

VIII CLAIMS APPENDIX

1 (Previously Presented) A method for controlling access to file on a server over a network, the method comprising:

(a) allowing a content originator to publish a file on a first server and to specify what users are authorized to access to file;

(b) replicating the file from the first server on a second server;

(c) in response to receiving a URL request from a client for a file from the first server, determining if a user of the client has been granted authorization to access the file, wherein a client address apparent to the first server differs from a client address apparent to the second server;

(d) generating a transfer ticket from the first server to the client that includes an identifier identifying the particular file on the second server if the user has been granted authorization access, wherein the transfer ticket is not bound to the client address apparent to the first server;

(e) in response to receiving the transfer ticket from the client by the second server, redirecting the client back to the second server with a URL ticket, wherein the URL ticket is bound to the client address apparent to the second server; and

(f) in response to receiving the URL ticket from the client, verifying the URL ticket on the second server and returning the file .

2 (Canceled)

3 (Original) The method of claim 1 wherein step (c) further includes the step of: using a web browser for the client, wherein the web browser has not been customized to request tickets.

4 (Original) The method of claim 1 wherein step (a) further includes the step of: allowing the content originator to specify what access privileges each user has with respect to the files, the access privileges including read, write, and delete.

5 (Original) The method of claim 4 wherein step (a) further includes the step of: allowing the access controls to be specified before and after the file is replicated onto the second server.

6 (Original) The method of claim 4 wherein step (a) further includes the steps of: storing the name of the file in a database along with access privileges specified for the file, and when a user makes a request to access the file, looking up the name of the file in the database and determining if the user has been granted access to the file.

7 (Canceled).

8 (Previously Presented) The method of claim 1 wherein step (e) further includes the step of: placing into the URL ticket a path parameter, a start parameter, a use-by parameter, an end parameter, a uid parameter, a clientid parameter, a sessionid parameter, a referrer parameter, and a message authentication code (MAC).

9 (Previously Presented) The method of claim 8 wherein step (e) further includes the step of: binding a combination of “basedir+path+sessionid” to an IP address of the client at first use of the URL ticket.

10 (Previously Presented) The method of claim 9 wherein step (e) further includes the step of: verifying the URL ticket as valid when;

(i) the MAC is correct,

(ii) a current time is between values of the start and use-by parameters, or the "basedir+path+sessionID" combination has previously been used for the same IP address,

(iii) the "basedir+path+sessionID" combination has not been used from a different IP address, and

(iv) the URL requests a file that is in a subtree rooted by basedir+”/”path.

11 (Canceled)

12 (Original) The method of claim 1 further including the step of providing a content server as the first server and providing at least one replica server as the second server.

13 (Previously Presented) A system for controlling access to file on a server over a network, the system comprising:

means for allowing a content originator to publish a file on a first server and to specify what users are authorized to access to the file, wherein files on the first server are replicated on a second server;

means responsive to receiving a URL request from a client for a file from the first server for determining if a user of the client has been granted authorization to access the file, wherein a client address apparent to the first server differs from a client address apparent to the second server;

means for generating a transfer ticket from the first server to the client that includes an identifier identifying the particular file on the second server if the user has been granted authorization access, wherein the transfer ticket is not bound to the client address apparent to the first server;

means for receiving the transfer ticket from the client by the second server and redirecting the client back to the second server with a URL ticket, wherein the URL ticket is bound to the client address apparent to the second server; and

means for verifying the URL ticket on the second server and returning the file.

14 (Canceled)

15 (Original) The system of claim 13 wherein the client comprises a web browser that has not been customized to request tickets.

16 (Original) The system of claim 13 wherein the content originator specifies what access privileges each user has with respect to the files, the access privileges including

read, write, and delete.

17 (Original) The system of claim 16 wherein the access controls can be specified before and after the file is replicated onto the second server.

18 (Original) The system of claim 16 wherein a name of the file is stored in a database along with the access privileges specified for the file, and when a user makes a request to access the file, the name of the file is looked up in the database to determine if the user has been granted access to the file.

19 (Canceled).

20 (Previously Presented) The system of claim 13 wherein the URL ticket includes a path parameter, a start parameter, a use-by parameter, an end parameter, a uid parameter, a clientid parameter, a sessionid parameter, a referrer parameter, and a message authentication code (MAC).

21 (Original) The system of claim 20 wherein a combination of "basedir+path+sessionid" is bound to an IP address of the client at first use of the URL ticket.

22 (Original) The system of claim 21 wherein the URL ticket is verified as valid when;

(i) the MAC is correct,

(ii) a current time is between values of the start and use-by parameters, or the "basedir+path+sessionID" combination has previously been used for the same IP address,

(iii) the "basedir+path+sessionID" combination has not been used from a different IP address, and

(iv) the URL requests a file that is in a subtree rooted by basedir+"/"path.

23 (Canceled)

24 (Original) The system of claim 13 wherein the first server comprises a content server and the second server comprises at least one replica server.

25 (Previously Presented) A computer-readable medium containing program instructions for controlling access to file on a server over a network, the program instructions for:

(a) allowing a content originator to publish a file on a first server and to specify what users are authorized to access to file;

(b) replicating the file from the first server on a second server;

(c) in response to receiving a URL request from a client for a file from the first server, determining if a user of the client has been granted authorization to access the file, wherein a client address apparent to the first server differs from a client address apparent to the second server;

(d) generating a transfer ticket that includes an identifier identifying the particular file on the second server if the user has been granted authorization access, wherein the transfer ticket is not bound to the client address apparent to the first server;

(e) in response to receiving the transfer ticket from the client by the second server, redirecting the client back to the second server with a URL ticket, wherein the URL ticket is bound to the client address apparent to the second server; and

(f) in response to receiving the URL ticket from the client, verifying the URl ticket on the second server and returning the file.

26 (Canceled)

27 (Previously Presented) The computer-readable medium of claim 25 wherein instruction (c) further includes the instruction of: using a web browser for the client, wherein the web browser has not been customized to request tickets.

28 (Previously Presented) The computer-readable medium of claim 25 wherein instruction (a) further includes the instruction of: allowing the content originator to specify what access privileges each user has with respect to the files, the access privileges including read, write, and delete.

29 (Previously Presented) The computer-readable medium of claim 28 wherein

instruction (a) further includes the instruction of: allowing the access controls to be specified before and after the file is replicated onto the second server.

30 (Previously Presented) The computer-readable medium of claim 28 wherein instruction (a) further includes the instructions of: storing the name of the file in a database along with access privileges specified for the file, and when a user makes a request to access the file, looking up the name of the file in the database and determining if the user has been granted access to the file.

31 (Canceled).

32 (Previously Presented) The computer-readable medium of claim 25 wherein instruction (e) further includes the instruction of: placing into the URL ticket a path parameter, a start parameter, a use-by parameter, an end parameter, a uid parameter, a clientid parameter, a sessionid parameter, a referrer parameter, and a message authentication code (MAC).

33 (Previously Presented) The computer-readable medium of claim 25 wherein instruction (e) further includes the instruction of: binding a combination of "basedir+path+sessionid" to an IP address of the client at first use of the URL ticket.

34 (Previously Presented) The computer-readable medium of claim 33 wherein instruction (g) further includes the instruction of: verifying the URL ticket as valid when;

(i) the MAC is correct,

(ii) a current time is between values of the start and use-by parameters, or the "basedir+path+sessionID" combination has previously been used for the same IP address,

(iii) the "basedir+path+sessionID" combination has not been used from a different IP address, and

(iv) the URL requests a file that is in a subtree rooted by basedir+"/"path.

35 (Canceled)

36 (Previously Presented) The computer-readable medium of claim 25 further including the instruction of providing a content server as the first server and providing at least one replica server as the second server.

37 (Canceled)

38 (Canceled)

IX EVIDENCE APPENDIX

(None)

X RELATED PROCEEDINGS APPENDIX

(None)